



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11212461 A**(43) Date of publication of application: **06 . 08 . 99**

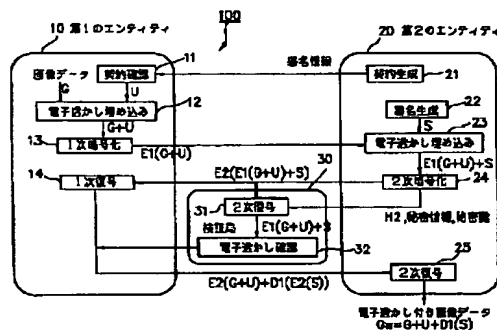
(51) Int. Cl. **G09C 5/00**
G09C 1/00
H04L 9/32
H04N 1/387
H04N 7/08
H04N 7/081

(21) Application number: **10013954**(22) Date of filing: **27 . 01 . 98**(71) Applicant: **CANON INC**(72) Inventor: **IWAMURA KEIICHI****(54) ELECTRONIC WATERMARK SYSTEM AND ELECTRONIC INFORMATION DELIVERY SYSTEM****(57) Abstract:**

PROBLEM TO BE SOLVED: To provide an electronic watermark system which surely prevents unauthorized copy of digital data related to copyright.

SOLUTION: The encryption processing and the electronic watermark burying processing of data are distributedly performed in first and second entities (including an author, a selling agent, and a user of data) 10 and 11, and the validity of these encryption processing and electronic watermark burying processing is verified in an independent entity (verification station) 30, thereby surely recognizing the wrong action at the time when the author, the selling agent, or the user wrongfully copies and delivers data. Since check is performed in the verification station in the stage of data delivery from the author to the selling agent and in the stage of that from the selling agent to the user, they cannot do wrong in league with each other, and a system safe against unauthorized delivery of data is realized.

COPYRIGHT: (C)1999,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-212461

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.⁶

識別記号

F I

G 0 9 C 5/00

G 0 9 C 5/00

1/00

6 4 0

1/00

6 4 0 C

H 0 4 L 9/32

H 0 4 N 1/387

H 0 4 N 1/387

H 0 4 L 9/00

6 7 5 D

7/08

H 0 4 N 7/08

Z

審査請求 未請求 請求項の数30 O L (全 24 頁) 最終頁に続く

(21) 出願番号

特願平10-13954

(22) 出願日

平成10年(1998) 1月27日

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 岩村 恵市

東京都大田区下丸子3丁目30番2号 キヤ

ノン株式会社内

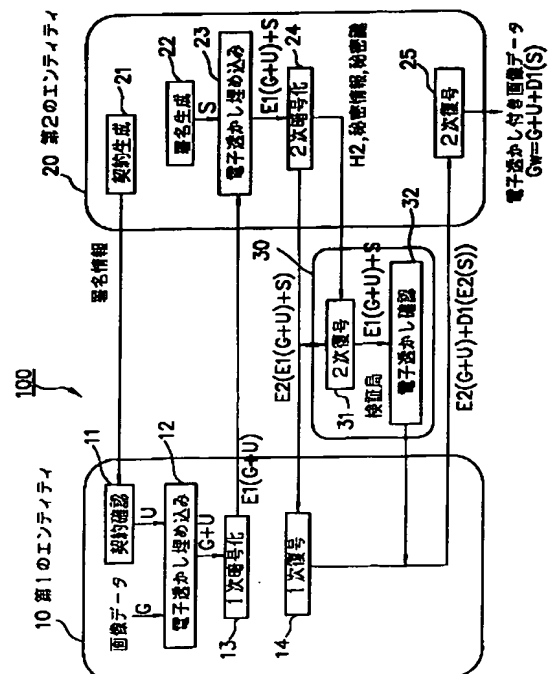
(74) 代理人 弁理士 國分 孝悦

(54) 【発明の名称】 電子透かし方式および電子情報配布システム

(57) 【要約】

【課題】 著作権に係るデジタルデータの不正コピーを確実に防止できる電子透かし方式を提供する。

【解決手段】 データに対する暗号処理および電子透かし埋め込み処理を第1、第2のエンティティ（データの著作者、販売代理店、ユーザを含む）10、11で分散して行い、上記暗号処理および電子透かし埋め込み処理の正当性を別個のエンティティ（検証局）30で検証するようにすることにより、著作者、代理店またはユーザがデータを不正にコピーして配布を行った際にその不正行為を確実に認識することができるようにする。また、このシステムでは、著作者から代理店にデータを渡す段階および代理店からユーザにデータを渡す段階のそれぞれにおいて検証局による検査が行われるので、結託して不正することはあり得ず、データの不正配布に関して安全なシステムを実現できる。



【特許請求の範囲】

【請求項 1】 データに対する暗号処理および電子透かし埋め込み処理を複数の手段またはエンティティで分散して行い、上記複数の手段またはエンティティで行われた上記暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を、上記複数の手段またはエンティティとは別の手段またはエンティティで検証することを特徴とする電子透かし方式。

【請求項 2】 上記複数の手段またはエンティティは、少なくとも 3 種以上の手段またはエンティティであることを特徴とする請求項 1 に記載の電子透かし方式。

【請求項 3】 上記複数の手段またはエンティティは、データに対して第 1 の暗号処理を行う手段を有する第 1 のエンティティと、
上記電子透かし埋め込み処理を行う手段を有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、
第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティとから成ることを特徴とする請求項 2 に記載の電子透かし方式。

【請求項 4】 上記複数の手段またはエンティティは、データに対して第 1 の暗号処理を行う手段を有する第 1 のエンティティと、
上記電子透かし埋め込み処理を行う手段を有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、
上記電子透かし埋め込み処理を行う手段および第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティとから成ることを特徴とする請求項 2 に記載の電子透かし方式。

【請求項 5】 上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第 1 の暗号処理を行う手段を有する第 1 のエンティティと、
上記電子透かし埋め込み処理を行う手段を有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、
第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティとから成ることを特徴とする請求項 2 に記載の電子透かし方式。

【請求項 6】 上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第 1 の暗号処理を行う手段を有する第 1 のエンティティと、
上記電子透かし埋め込み処理を行う手段、第 1 の暗号処理を行う手段および第 2 の暗号処理を行う手段の少なくとも 1 つを有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、
上記電子透かし埋め込み処理を行う手段および第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用

する第 3 のエンティティとから成ることを特徴とする請求項 2 に記載の電子透かし方式。

【請求項 7】 上記エンティティは、電子透かしの埋め込まれたデータに対して暗号化を行うことを特徴とする請求項 1 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 8】 上記エンティティは、暗号化の施されたデータに対して電子透かしの埋め込むことを特徴とする請求項 1 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 9】 上記第 2 のエンティティは、上記第 1 のエンティティからの上記第 1 の暗号処理が施されたデータに対して電子透かしの埋め込むことを特徴とする請求項 3 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 10】 上記第 2 のエンティティは、上記第 1 のエンティティからの上記第 1 の暗号処理が施されたデータおよび上記第 3 のエンティティからの上記第 2 の暗号処理が施されたデータに対して電子透かしの埋め込むことを特徴とする請求項 3 に記載の電子透かし方式。

【請求項 11】 上記第 2 のエンティティは、上記第 2 の暗号処理が施されたデータを一方方向性関数により変換した値を出力することを特徴とする請求項 10 に記載の電子透かし方式。

【請求項 12】 上記第 2 のエンティティは、上記一方方向性関数により変換した値を上記第 4 のエンティティに送信することを特徴とする請求項 11 に記載の電子透かし方式。

【請求項 13】 上記第 3 のエンティティは、上記第 2 の暗号処理が施されたデータを一方方向性関数により変換した値を上記第 2 の暗号処理が施されたデータと共に出力することを特徴とする請求項 3 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 14】 上記第 3 のエンティティは、上記一方方向性関数により変換した値を上記第 4 のエンティティに送信することを特徴とする請求項 13 に記載の電子透かし方式。

【請求項 15】 上記第 3 のエンティティは、あらかじめ一次暗号化された情報を受け取り、該暗号化された情報に対して二次暗号化を施すことを特徴とする請求項 3 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 16】 上記第 4 のエンティティは、上記第 2 の暗号処理に対応する復号処理を行うことが可能であることを特徴とする請求項 3 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 17】 上記第 4 のエンティティは、暗号鍵を管理する手段を有することを特徴とする請求項 3 ～ 6 の何れか 1 項に記載の電子透かし方式。

【請求項 18】 上記第 4 のエンティティは、他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを復号化することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証することを特徴とする請求項 17 に記載の電子透かし方式。

【請求項 19】 上記第 4 のエンティティは、上記他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを一方方向性関数で変換した値と、上記他のエンティティから出力される値とを比較することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証することを特徴とする請求項 17 または 18 に記載の電子透かし方式。

【請求項 20】 複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して第 1 の暗号処理を行う手段を有する第 1 のエンティティと、電子透かし埋め込み処理を行う手段を有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティと、上記第 1 ～第 3 のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第 4 のエンティティとを有することを特徴とする電子情報配信システム。

【請求項 21】 複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して第 1 の暗号処理を行う手段を有する第 1 のエンティティと、電子透かし埋め込み処理を行う手段を有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、上記電子透かし埋め込み処理を行う手段および第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティと、上記第 1 ～第 3 のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第 4 のエンティティとを有することを特徴とする電子情報配信システム。

【請求項 22】 複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して電子透かし埋め込み処理を行う手段および第 1 の暗号処理を行う手段を有する第 1 のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティと、上記第 1 ～第 3 のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第 4 のエンティティとを有することを特徴とす

る電子情報配信システム。

【請求項 23】 複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して電子透かし埋め込み処理を行う手段および第 1 の暗号処理を行う手段を有する第 1 のエンティティと、上記電子透かし埋め込み処理を行う手段、第 1 の暗号処理を行う手段および第 2 の暗号処理を行う手段の少なくとも 1 つを有し、上記第 1 のエンティティからのデータを管理および配付する第 2 のエンティティと、上記電子透かし埋め込み処理を行う手段および第 2 の暗号処理を行う手段を有し、電子透かし付きデータを利用する第 3 のエンティティと、上記第 1 ～第 3 のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第 4 のエンティティとを有することを特徴とする電子情報配信システム。

【請求項 24】 上記検証を行う第 4 のエンティティは、暗号鍵を管理するエンティティであることを特徴とする請求項 20 ～ 23 の何れか 1 項に記載の電子情報配布システム。

【請求項 25】 上記第 1 のエンティティが埋め込む電子透かし情報は、上記第 3 のエンティティに関する情報を含むことを特徴とする請求項 22 または 23 に記載の電子情報配布システム。

【請求項 26】 上記第 1 のエンティティが埋め込む電子透かし情報は、送信するデジタルデータに関する情報を含むことを特徴とする請求項 22 または 23 に記載の電子情報配布システム。

【請求項 27】 上記第 2 のエンティティが埋め込む電子透かし情報は、上記第 3 のエンティティに関する情報を含むことを特徴とする請求項 20 ～ 23 の何れか 1 項に記載の電子情報配布システム。

【請求項 28】 上記第 3 のエンティティが埋め込む電子透かし情報は、上記第 3 のエンティティのみが作成できる情報であることを特徴とする請求項 21 または 23 に記載の電子情報配布システム。

【請求項 29】 上記第 1 のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第 3 のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うことを特徴とする請求項 22 または 23 に記載の電子情報配布システム。

【請求項 30】 上記第 2 のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第 3 のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うことを特徴とする請求項 20 ～ 23 の何れか 1 項に記載の電子情報配布システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は電子透かし方式および電子情報配布システムに関し、特に、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等のデジタル情報における著作権を保護するための電子透かし技術、およびそれを用いてデジタル情報の配布を行うマルチメディアネットワークに用いて好適なものである。

【0002】

【従来の技術】近年のコンピュータネットワークの発達と、安価で高性能なコンピュータの普及とにより、ネットワーク上で商品の売買を行う電子商取引が盛んになってきている。そこで取引される商品として、例えば画像等を含むデジタルデータが考えられる。しかし、デジタルデータは、完全なコピーを容易かつ大量に作成できるという性質を持ち、これは、そのデジタルデータを買ったユーザがオリジナルと同質のコピーを不正に作成して再配布できるという可能性を示す。これにより、本来デジタルデータの著作権または著作権から正当に販売を委託された者（以下、「販売者」と言う）に支払われるべき代価が支払われず、著作権が侵害されていると考えられる。

【0003】一方、著作権または販売者（以下、これらのデジタルデータを正当に配布する者をまとめて「サーバ」と言う）がユーザにデジタルデータを一度送ってしまうと、上述の不正コピーを完全に防止することはできない。そのため、不正コピーを直接防止するのではなく、電子透かしと呼ばれる手法が提案されている。この電子透かしとは、オリジナルのデジタルデータにある操作を加え、デジタルデータに関する著作権情報やユーザに関する利用者情報をデジタルデータ中に埋め込むことによって、不正コピーが見つかった場合に誰がデータを再配布したのかを特定する手法である。

【0004】従来の電子透かしを用いたシステムでは、サーバは完全に信頼できる機関であることが前提となっている。よって、もしサーバが信頼できる機関ではなく不正を行う可能性があるとする、従来のシステムでは不正コピーを行っていないユーザに罪が押し付けられてしまう場合が存在する。

【0005】これは、図13に示すように、従来のシステムでは、ユーザを特定するための利用者情報d1をデジタルデータ（以下、デジタルデータを画像データとして説明する）gにサーバが埋め込むので、サーバが勝手に利用者情報d1を埋め込んでそのコピーを不正に配布した場合、その利用者情報d1から特定されるユーザは、サーバの主張を退ける手段がないためである。

【0006】その対策として、例えば、「B.Pfitmann and M.Waidner: "Asymmetric Fingerprinting," EUROCRYPT'96」の文献（以下、文献[1]と記す）に、公開鍵暗号方式を用いたシステム（図14）が提案されている。ここで、公開鍵暗号方式とは、暗号鍵と復号鍵が異な

り、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。その代表例として、RSA暗号やElGamal暗号等が知られている。以下、公開鍵暗号方式における（a）特徴、（b）秘密通信や認証通信等のプロトコルについて述べる。

【0007】（a）公開鍵暗号の特徴

（1）暗号鍵と復号鍵とが異なり、暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（2）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（3）送られてきた通信文の送信者が偽者でないこと、およびその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【0008】（b）公開鍵暗号のプロトコル

例えば、通信文Mに対して、公開の暗号鍵kpを用いて行う暗号化操作をE(kp, M)とし、秘密の復号鍵ksを用いて行う復号操作をD(ks, M)とすると、公開鍵暗号アルゴリズムは、まず次の2つの条件を満たす。

（1）暗号鍵kpが与えられたとき、暗号化操作E(kp, M)の計算は容易である。また、復号鍵ksが与えられたとき、復号操作D(ks, M)の計算は容易である。

（2）もしユーザが復号鍵ksを知らないなら、暗号鍵kpと、暗号化操作E(kp, M)の計算手順と、暗号文C=E(kp, M)とを知っていても、通信文Mを決定することは計算量の点で困難である。

【0009】次に、上記（1）、（2）の条件に加えて、次の（3）の条件が成立することにより秘密通信機能が実現できる。

（3）全ての通信文（平文）Mに対し暗号化操作E(kp, M)が定義でき、

$$D(ks, E(kp, M)) = M$$

が成立する。つまり、暗号鍵kpは公開されているため、誰もが暗号化操作E(kp, M)の計算を行うことができるが、D(ks, E(kp, M))の計算をして通信文Mを得ることができるのは、秘密の復号鍵ksを持っている本人だけである。

【0010】一方、上記（1）、（2）の条件に加えて、次の（4）の条件が成立することにより認証通信機能が実現できる。

（4）全ての通信文（平文）Mに対し復号操作D(ks, M)が定義でき、

$$E(kp, D(ks, M)) = M$$

が成立する。つまり、復号操作D(ks, M)の計算ができるのは秘密の復号鍵ksを持っている本人のみであり、他の人が偽の秘密の復号鍵ks'を用いてD(ks', M)の計算を行い、秘密の復号鍵ksを持っている本人になりすましたとしても、

$E(k_p, D(k_{s'}, M)) \neq M$

であるため、受信者は受けとった情報が不正なものであることを確認できる。また、 $D(k_s, M)$ の値が改ざんされても、

$E(k_p, D(k_s, M)') \neq M$

となり、受信者は受けとった情報が不正なものであることを確認できる。

【0011】上述のような公開鍵暗号方式では、公開の暗号鍵（以下、公開鍵とも言う） k_p を用いる処理 $E()$ を「暗号化」、秘密の復号鍵（以下、秘密鍵とも言う） k_s を用いる処理 $D()$ を「復号」と呼んでいる。したがって、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【0012】以下に、公開鍵暗号方式により送信者Aから受信者Bへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。ここで、送信者Aの秘密鍵を k_{sA} 、公開鍵を k_{pA} とし、受信者Bの秘密鍵を k_{sB} 、公開鍵を k_{pB} とする。

【0013】[秘密通信]送信者Aから受信者Bへ通信文（平文） M を秘密通信する場合は、次の手順で行う。

Step 1：送信者Aは、受信者Bの公開鍵 k_{pB} で通信文 M を以下のように暗号化し、暗号文 C を受信者Bに送る。

$C = E(k_{pB}, M)$

Step 2：受信者Bは、自分の秘密鍵 k_{sB} で暗号文 C を以下のように復号し、もとの平文 M を得る。

$M = D(k_{sB}, C)$

なお、受信者Bの公開鍵 k_{pB} は不特定多数に公開されているので、送信者Aに限らず全ての人が受信者Bに秘密通信できる。

【0014】[認証通信]送信者Aから受信者Bへ通信文（平文） M を認証通信する場合は、次の手順で行う。

Step 1：送信者Aは、自分の秘密鍵 k_{sA} で送信文 S を以下のように生成し、受信者Bに送る。

$S = D(k_{sA}, M)$

この送信文 S を「署名文」と言い、署名文 S を得る操作を「署名」と言う。

Step 2：受信者Bは、送信者Aの公開鍵 k_{pA} で署名文 S を以下のように復元変換し、もとの平文 M を得る。

$M = E(k_{pA}, S)$

もし、通信文 M が意味のある文であることを確認したならば、通信文 M が確かに送信者Aから送られてきたことを認証する。送信者Aの公開鍵 k_{pA} は不特定多数に公開されているので、受信者Bに限らず全ての人が送信者Aの署名文 S を認証できる。このような認証を「デジタル署名」とも言う。

【0015】[署名付秘密通信]送信者Aから受信者Bへ通信文（平文） M を署名付秘密通信する場合は、次の手順で行う。

Step 1：送信者Aは、自分の秘密鍵 k_{sA} で通信文 M を以下のように署名し、署名文 S を作る。

$S = D(k_{sA}, M)$

さらに、送信者Aは、受信者Bの公開鍵 k_{pB} で署名文 S を以下のように暗号化し、暗号文 C を受信者Bに送る。

$C = E(k_{pB}, S)$

Step 2：受信者Bは、自分の秘密鍵 k_{sB} で暗号文 C を以下のように復号し、署名文 S を得る。

$S = D(k_{sB}, C)$

さらに、受信者Bは、送信者Aの公開鍵 k_{pA} で署名文 S を以下のように復元変換し、もとの平文 M を得る。

$M = E(k_{pA}, S)$

もし、通信文 M が意味のある文であることを確認したならば、通信文 M が確かに送信者Aから送られてきたことを認証する。

【0016】なお、署名付秘密通信の各Step内における関数を施す順序は、それぞれ逆転しても良い。すなわち、上述の手順では、

Step 1： $C = E(k_{pB}, D(k_{sA}, M))$

Step 2： $M = E(k_{pA}, D(k_{sB}, C))$

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Step 1： $C = D(k_{sA}, E(k_{pB}, M))$

Step 2： $M = D(k_{sB}, E(k_{pA}, C))$

【0017】以下に、上述のような公開鍵暗号方式を適用した従来の電子透かしを用いるシステム（上記図14）における操作の手順を示す。

1）まず、サーバとユーザ間で画像データ g の売買に関する契約書 d_2 を取り交わす。

【0018】2）次に、ユーザは、自分を示す乱数 ID を発生させ、これを用いて一方向性関数 f を生成する。この一方向性関数とは、関数 $y = f(x)$ において、 x から y を求めることは容易だが、逆に y から x を求めることが困難な関数を言う。例えば、桁数の大きな整数に対する素因数分解や離散対数等が一方向性関数としてよく用いられる。

3）次に、ユーザは、契約書 d_2 と一方向性関数 f に対して、自分の秘密鍵 k_{sU} を用いて署名情報 d_3 を生成し、それらを合わせてサーバに送る。

【0019】4）次に、サーバは、ユーザの公開鍵 k_{pU} を用いて署名情報 d_3 と契約書 d_2 を確認する。

5）サーバは確認後、現在までの全配布記録 d_4 と、ユーザが作成した乱数 ID とを画像データ g に埋め込み、電子透かし付き画像データ（ $g + d_4 + ID$ ）を生成する。

6）サーバは、ユーザにその電子透かし付き画像データ（ $g + d_4 + ID$ ）を送る。

【0020】この後、不正コピーが発見された場合は、その不正画像データから埋め込み情報を抽出し、そこに

含まれるIDからユーザを特定する。このとき、その不正コピーがサーバによって無断で配布されたものでないことは、以下のことを根拠として主張される。それは、ユーザを特定するIDはユーザ自身によって生成され、それを用いた一方向性関数値 f にユーザの署名が付けられるので、サーバは任意のユーザに対してそのようなIDを生成できないということである。しかし、サーバとの間で正式に契約したユーザは自分を特定するIDをサーバに送るために、正式に契約したユーザへの罪の押し付けはやはり可能であり、契約していないユーザへの罪の押し付けが不可能になるだけである。

【0021】そこで、正式に契約したユーザにも罪の押し付けが不可能になるシステム(図15)が、「三浦、渡辺、嵩(奈良先端大):“サーバの不正も考慮した電子透かしについて”, SCIS97-31C」の文献(以下、文献[2]と記す)に提案されている。これは、サーバを原画像サーバと埋め込みサーバに分割することによって実現される。ただし、このシステムでは、暗号化時および復号時において、埋め込まれた電子透かしは壊されないとしている。以下、上記図15のシステムにおける操作の

手順を示す。

【0022】1) まず、ユーザが原画像サーバに所望の画像データを、署名 d_5 を付けて要求する。
2) 原画像サーバは、その要求内容をユーザの署名 d_5 から確認し、その確認後に、要求された画像データ g を暗号化して埋め込みサーバに送る。このとき、原画像サーバは、ユーザ名 u および委託内容 d_6 に対する署名を付けて埋め込みサーバに送る。これと同時に、原画像サーバは、暗号化に対する復号関数 f' をユーザに送る。

【0023】3) 埋め込みサーバは、送られてきた暗号化画像データ g' と、署名 $(u + d_6)$ とを確認し、ユーザ名 u および委託内容 d_6 を基にユーザを特定する利用者情報 d_7 の作成および埋め込みを行い、電子透かし付き暗号化画像データ $(g' + d_7)$ を作成する。その後、埋め込みサーバは、その電子透かし付き暗号化画像データ $(g' + d_7)$ をユーザに送る。

4) ユーザは、原画像サーバから送られてきた復号関数 f' を用いて、電子透かし付き暗号化画像データ $(g' + d_7)$ を電子透かし付き画像データ $(g + d_7)$ へと復号する。

【0024】この後、不正コピーが発見された場合は、原画像サーバはその不正画像データを暗号化して埋め込み情報を抽出し、それを埋め込みサーバに送る。埋め込みサーバは、この埋め込み情報からユーザを特定する。このシステムでは、原画像サーバはユーザを特定するための利用者情報 d_7 を画像データ g に埋め込んでおらず、また、埋め込みサーバは復号関数 f' を知らない(画像を元に戻せない)ので、正式に契約したユーザに対しても、各サーバはユーザの利用者情報 d_7 を無断で埋め込んだ画像データを不正配布できないことを根拠に

している。

【0025】しかしながら、この図15のシステムでは、原画像サーバと埋め込みサーバとの結託については考慮せず、埋め込みサーバとユーザとの結託も考えていない。よって、埋め込みサーバが原画像である画像データ g の暗号化画像データ g' を持ち、ユーザが復号関数 f' を持つため、原画像サーバと埋め込みサーバとが結託した場合には、上述の図14のシステムと同様にサーバの不正が可能であるし、埋め込みサーバとユーザとが結託した場合には原画像の不正入手が可能である。

【0026】また、原画像サーバは復号関数 f' をユーザに送るが、ユーザの復号関数 f' の管理が不十分であれば、埋め込みサーバはユーザと結託しなくてもユーザの不注意等から復号関数 f' を知ることができる可能性は大きい。

【0027】さらに、このシステムでは、原画像サーバは埋め込み手段を有しない、または正しい埋め込みができないとしているが、埋め込み情報を抽出するのは原画像サーバであるので、埋め込み情報を解析すれば、原画像サーバが正しい埋め込みを行えるようになる可能性は高いと考えられる。そして、この場合、上述の図14のシステムと同様の不正が可能である。

【0028】さらに、上述のように従来はユーザとサーバとからなるシステムが不完全ながら提案されていたが、画像データの売買に関係する要素が階層的に構成される場合における安全なシステムは提案されていなかった。階層的なシステムの例としては、図16に示すように、サーバの下に複数の代理店があり、その下にユーザがあるといったシステムであったり、図17に示すように、ある販売代理店に複数の著作家が自分の著作に係る画像データの販売を依頼し、その依頼を受けた代理店が複数の著作家の画像データを多くのユーザに販売するといったシステムとして考えられる。

【0029】これらの階層的なシステムにおいては、画像データの売買を構成する要素が上述のサーバおよびユーザの二者からサーバ(または著作家)、代理店およびユーザの三者に増えるために、結託の問題などは構成要素が二者のシステムよりも複雑になる。すなわち、上記図15のシステムは広く考えると、サーバと代理店とユーザとが構成要素のシステムであるとも考えられるが、文献[2]は階層的なシステムを想定したものではなく、1つのサーバの不正を防止するという観点からサーバを分割したものであり、上述のように結託の問題も考慮していない。

【0030】

【発明が解決しようとする課題】本発明はこのような実情に鑑みて成されたものであり、上述のような不正を確実に防止できる電子透かし方式および電子情報配布システムを提供することを目的とする。特に本発明は、著作物の売買に関係する要素が階層的に構成されているシス

テムにおいて、結託による不正を確実に防止できるようにすることを目的としている。

【0031】

【課題を解決するための手段】本発明の電子透かし方式は、データに対する暗号処理および電子透かし埋め込み処理を複数の手段またはエンティティで分散して行い、上記複数の手段またはエンティティで行われた上記暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を、上記複数の手段またはエンティティとは別の手段またはエンティティで検証することを特徴とする。

ここで、上記複数の手段またはエンティティは、少なくとも3種以上の手段またはエンティティであっても良い。

【0032】例えば、上記複数の手段またはエンティティは、データに対して第1の暗号処理を行う手段を有する第1のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティとから成るものであっても良い。

【0033】また、上記複数の手段またはエンティティは、データに対して第1の暗号処理を行う手段を有する第1のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティとから成るものであっても良い。

【0034】また、上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第1の暗号処理を行う手段を有する第1のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、上記電子透かし埋め込み処理を行う手段および第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティとから成るものであっても良い。

【0035】さらに、上記複数の手段またはエンティティは、データに対して上記電子透かし埋め込み処理を行う手段および第1の暗号処理を行う手段を有する第1のエンティティと、上記電子透かし埋め込み処理を行う手段、第1の暗号処理を行う手段および第2の暗号処理を行う手段の少なくとも1つを有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、上記電子透かし埋め込み処理を行う手段および第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティとから成るものであっても良い。

【0036】上記の構成において、上記エンティティは、電子透かしの埋め込まれたデータに対して暗号化を

行うようにしても良い。また、上記エンティティは、暗号化の施されたデータに対して電子透かしを埋め込むようにしても良い。

【0037】また、上記第2のエンティティは、上記第1のエンティティからの上記第1の暗号処理が施されたデータに対して電子透かしを埋め込むようにしても良い。また、上記第2のエンティティは、上記第1のエンティティからの上記第1の暗号処理が施されたデータおよび上記第3のエンティティからの上記第2の暗号処理が施されたデータに対して電子透かしを埋め込むようにしても良い。また、上記第2のエンティティは、上記第2の暗号処理が施されたデータを一方向性関数により変換した値を出力するようにしても良い。また、上記第2のエンティティは、上記一方向性関数により変換した値を上記第4のエンティティに送信するようにしても良い。

【0038】また、上記第3のエンティティは、上記第2の暗号処理が施されたデータを一方向性関数により変換した値を上記第2の暗号処理が施されたデータと共に出力するようにしても良い。また、上記第3のエンティティは、上記一方向性関数により変換した値を上記第4のエンティティに送信するようにしても良い。また、上記第3のエンティティは、あらかじめ一次暗号化された情報を受け取り、該暗号化された情報に対して二次暗号化を施すようにしても良い。

【0039】また、上記第4のエンティティは、上記第2の暗号処理に対応する復号処理を行うことが可能であるようにしても良い。また、上記第4のエンティティは、暗号鍵を管理する手段を有するようにしても良い。また、上記第4のエンティティは、他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを復号化することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証するようにしても良い。また、上記第4のエンティティは、上記他のエンティティから出力される暗号化され電子透かしが埋め込まれたデータを一方向性関数で変換した値と、上記他のエンティティから出力される値とを比較することにより、上記電子透かしおよび暗号処理の少なくとも一方の正当性を検証するようにしても良い。

【0040】また、本発明の電子情報配布システムは、複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して第1の暗号処理を行う手段を有する第1のエンティティと、電子透かし埋め込み処理を行う手段を有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティと、上記第1～第3のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第4のエンティ

ティとを有することを特徴とする。

【0041】本発明の他の態様では、複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して第1の暗号処理を行う手段を有する第1のエンティティと、電子透かし埋め込み処理を行う手段を有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、上記電子透かし埋め込み処理を行う手段および第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティと、上記第1～第3のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第4のエンティティとを有することを特徴とする。

【0042】本発明のその他の態様では、複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して電子透かし埋め込み処理を行う手段および第1の暗号処理を行う手段を有する第1のエンティティと、上記電子透かし埋め込み処理を行う手段を有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティと、上記第1～第3のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第4のエンティティとを有することを特徴とする。

【0043】本発明のその他の態様では、複数のエンティティからなるネットワークシステム上でデジタルデータの送受信を行う電子情報配布システムにおいて、データに対して電子透かし埋め込み処理を行う手段および第1の暗号処理を行う手段を有する第1のエンティティと、上記電子透かし埋め込み処理を行う手段、第1の暗号処理を行う手段および第2の暗号処理を行う手段の少なくとも1つを有し、上記第1のエンティティからのデータを管理および配付する第2のエンティティと、上記電子透かし埋め込み処理を行う手段および第2の暗号処理を行う手段を有し、電子透かし付きデータを利用する第3のエンティティと、上記第1～第3のエンティティで行われた暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を検証する第4のエンティティとを有することを特徴とする。

【0044】ここで、上記検証を行う第4のエンティティは、暗号鍵を管理するエンティティであっても良い。また、上記第1のエンティティが埋め込む電子透かし情報は、上記第3のエンティティに関する情報を含んでも良い。また、上記第1のエンティティが埋め込む電子透かし情報は、送信するデジタルデータに関する情報を含んでも良い。また、上記第2のエンティティが埋め込む電子透かし情報は、上記第3のエンティティに関する

情報を含んでも良い。また、上記第3のエンティティが埋め込む電子透かし情報は、上記第3のエンティティのみが作成できる情報であっても良い。また、上記第1のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第3のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うようにしても良い。また、上記第2のエンティティは、認証局によって発行される証明書付匿名公開鍵によって上記第3のエンティティの署名を検証した後に上記電子透かし埋め込み処理を行うようにしても良い。

【0045】

【発明の実施の形態】〔第1の実施形態〕以下、本発明に係る第1の実施形態を、図1を参照して説明する。本発明に係る電子透かし方式は、例えば、図1に示すようなシステム100により実施され、このシステム100は、本発明に係る電子情報配布システムを適用したものである。

【0046】すなわち、システム100は、第1のエンティティ側の端末装置（以下、第1端末装置と記す）10、第2のエンティティ側の端末装置（以下、第2端末装置と記す）20および検証局側の端末装置（以下、検証局端末装置と記す）30を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにデジタルデータの授受を行うようになされている。

【0047】第1端末装置10は、第2端末装置20からのデータが供給される契約確認処理部11と、例えば画像データ（デジタルデータ）および契約確認処理部11の出力が供給される電子透かし埋め込み処理部12と、電子透かし埋め込み処理部12の出力が供給される1次暗号化処理部13と、第2端末装置20からのデータが供給される1次復号処理部14とを備えており、1次暗号化処理部13および1次復号処理部14の各出力が第2端末装置20に送信されるようになされている。

【0048】また、第2端末装置20は、第1端末装置10の契約確認処理部11に対してデータを送信する契約生成処理部21と、署名生成処理部22と、署名生成処理部22および第1端末装置10の1次暗号化処理部13からのデータが供給される電子透かし埋め込み処理部23と、電子透かし埋め込み処理部23の出力が供給される2次暗号化処理部24と、第1端末装置10の1次復号処理部14からのデータが供給される2次復号処理部25とを備えており、2次復号処理部25の出力が電子透かし付き画像データとして出力されるようになされている。また、2次暗号化処理部24の出力は、第1端末装置10の1次復号処理部14および検証局端末装置30に各々供給されるようになされている。

【0049】また、検証局端末装置30は、第2端末装置20の2次暗号化処理部24からのデータが供給される2次復号処理部31と、2次復号処理部31の出力が

供給される電子透かし確認処理部32とを備えており、電子透かし確認処理部32の出力が第1端末装置10と第2端末装置20とに供給されるようになされている。また、2次復号処理部31の出力は、第1端末装置10の1次復号処理部14にも供給されるようになされている。

【0050】上記のように構成された本実施形態の電子情報配布システムにおいて、以下では、図16または図17に示したサーバまたは著作者が代理店にデジタルデータを渡す際の第1の埋込処理と、代理店がユーザにデジタルデータを渡す際の第2の埋込処理とに分けて考える。本実施形態は、第1の埋込処理と第2の埋込処理とを下記に示す同じプロトコルを用いて実現する。全体の処理は、第1の埋込処理を行った後に第2の埋込処理を行う。

【0051】下記の説明において、第1の埋込処理では上述の第1のエンティティはサーバまたは著作者を意味し、第2のエンティティは代理店を意味する。また、第2の埋込処理では第1のエンティティは代理店を意味し、第2のエンティティはユーザを意味する。したがって、少なくとも代理店において使用する端末装置は、図1の第1端末装置10と第2端末装置20に備えられた各処理部を全て有するものである。

【0052】上記第1の埋込処理および第2の埋込処理を実現する具体的なプロトコルを、図1を参照しながら以下に説明する。このプロトコルにおいて、方式や秘密鍵等の1次暗号に関する情報は第1のエンティティだけが知る情報であり、2次暗号に関する情報は第2のエンティティだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下、暗号化を「Ei()」、復号を「Di()」で表わし、電子透かしに関する埋め込み処理を「+」で表わすものとする。

【0053】以下に、上記のように構成したシステム100の動作を説明する。まず、電子透かしに関する埋め込み処理について説明する。

【0054】[埋め込み処理]

1) まず、第2端末装置20において、第2のエンティティが署名を付けて第1端末装置10(第1のエンティティ)に所望の画像データを要求する。この要求データは、契約生成処理部21により生成された署名情報であり、以下ではこれを契約情報と呼ぶ。

【0055】2) 次に、第1端末装置10において第1のエンティティは、契約確認処理部11を用いて受信した契約情報を第2のエンティティの署名から確認し、その確認後に、契約情報から利用者情報Uを作成する。そして、電子透かし埋め込み処理部12は、上記契約確認処理部11で作成された利用者情報Uを要求された画像データGに埋め込む。また、1次暗号化処理部13は、

電子透かし埋込処理部12で利用者情報Uが埋め込まれた画像データ(G+U)に対して1次暗号化処理E1()を行い、得られたデータを第2端末装置20に送る。よって、第2端末装置20には、1次暗号化画像データE1(G+U)の情報が送られることになる。

【0056】3) 次に、第2端末装置20において、署名生成処理部22は、第2のエンティティの秘密鍵を用いて署名情報Sを生成する。そして、電子透かし埋め込み処理部23は、署名生成処理部22で生成された署名情報Sを、第1端末装置10から送られてきた(配布された)1次暗号化画像データE1(G+U)に埋め込む。また、2次暗号化処理部24は、電子透かし埋め込み処理部23で署名情報Sが埋め込まれた1次暗号化画像データE1(G+U)+Sを2次暗号化して検証局端末装置30に送る。よって、検証局端末装置30には、2次暗号化画像データE2(E1(G+U)+S)の情報が送られることになる。

【0057】このとき、2次暗号化処理部24は、検証局端末装置30への送信データ(2次暗号化画像データE2(E1(G+U)+S))に対するハッシュ値H2を生成および署名し、署名情報Sを除く電子透かしに関連する秘密情報と、2次暗号化の秘密鍵とを共に検証局端末装置30に送る。なお、秘密情報とは、電子透かしを検出するための埋め込み位置や強度に関する情報であり、検証局端末装置30と共有している他の暗号方式によって暗号化して送られるものである。

【0058】また、ハッシュ値とは、一般にハッシュ関数h()の出力値であり、ハッシュ関数とは衝突を起こしにくい圧縮関数をいう。ここで、衝突とは、異なる値x1, x2に対してh(x1)=h(x2)となることである。また、圧縮関数とは、任意のビット長のビット列をある長さのビット列に変換する関数である。したがって、ハッシュ関数とは、任意のビット長のビット列をある長さのビット列に変換する関数h()で、h(x1)=h(x2)を満たす値x1, x2を容易に見出せないものである。このとき、任意の値yからy=h(x)を満たす値xを容易に見出せないのも、必然的にハッシュ関数は一方向性関数となる。このハッシュ関数の具体例としては、MD(Message Digest)5やSHA(Secure Hash Algorithm)等が知られている。

【0059】4) 次に、検証局端末装置30では、第2端末装置20から送られてきたハッシュ値H2の署名と、そのハッシュ値H2が送信データのハッシュ値と一致することを確認し、その確認後に2次復号処理部31は、第2端末装置20からの2次暗号化画像データE2(E1(G+U)+S)を復号し、そこから署名情報Sを抽出する。そして、電子透かし確認処理部32で署名情報Sを検査し、正しければ検証情報を作成して検証局端末装置30の署名を付ける。最後に、検証局端末装置30は、第2端末装置20から送信された2次暗号化

画像データE2 (E1 (G+U) + S) の情報とハッシュ値H2とその署名、およびそれに対する検証情報とその署名とを第1端末装置10に送る。

【0060】5) 次に、第1端末装置10において、第1のエンティティは、検証局端末装置30から送られてきた検証情報とその署名とを確認し、さらに2次暗号化画像データE2 (E1 (G+U) + S) とハッシュ値H2とその署名とを確認する。その確認後に1次復号処理部14は、上記2次暗号化画像データE2 (E1 (G+U) + S) の1次暗号化を復号してE2 (G+U) + D1 (E2 (S)) の情報を生成し、それを第2端末装置20に送る。

【0061】6) 次に、第2端末装置20において、2次復号処理部25は、第1端末装置10から送られてきたE2 (G+U) + D1 (E2 (S)) の情報の2次暗号化を復号して電子透かし付き画像データGwを取り出す。よって、電子透かし付き画像データGwは、 $Gw = G + U + D1 (S)$ と表わされる。これは、もとの画像データGに対して利用者情報Uと1次復号の影響を受けた第2のエンティティの署名情報Sとが透かし情報として埋め込まれていることを示す。

【0062】もし、第1のエンティティまたは第2のエンティティのどちらかの不正によって上記4)の過程において正しい透かし情報が検証局端末装置30で検証されない場合、そのことが第1端末装置10と第2端末装置20とに知らせられる。この時点で取り引きが中止されても、第1のエンティティは代価を得られないが画像データを第2のエンティティに不正入手されず、第2のエンティティは画像データを入手できないが第1のエンティティに代価を支払うことはない。したがって、第1のエンティティおよび第2のエンティティのどちらも、利益も不利益もなく不正をする意味がない。

【0063】すなわち、上記の電子透かし埋め込み処理を実行すれば、第1の埋込処理において第2のエンティティである代理店は、第1のエンティティであるサーバまたは原作者の原画像データGに対して自分の署名情報Sを埋め込んだ電子透かし付き画像データGwを得ることができる。なお、第1の埋込処理における利用者情報および署名情報をそれぞれU1, S1とすると、代理店が得る電子透かし付き画像データGwは、 $Gw = G + U1 + D1 (S1)$ となる。

【0064】次に、第2の埋込処理において、代理店の得た電子透かし付き画像データGwを原画像として同様の埋め込み処理を行えば(代理店を第1のエンティティとする)、このとき第2のエンティティとなるユーザは、電子透かし付き画像データGww= $G + U1 + D1 (S1) + U2 + D3 (S2)$ を得ることができる。ただし、第2の埋込処理における利用者情報および署名情報をそれぞれU2, S2とし、代理店が行う暗号化をE3 ()、復号をD3 ()で表わすものとする。

【0065】不正コピー(不正画像)が発見された場合は、以下のような簡単な検証処理で不正者を容易に特定できる。以下に述べる検証処理も、第1の埋込処理に対応するサーバまたは原作者と代理店間の検証処理である第1の検証処理と、第2の埋込処理に対応する代理店とユーザ間の検証処理である第2の検証処理とに分けて行う。その順番は、まず第1の検証処理を行い、次に第2の検証処理を行う。

【0066】ただし、第1の検証処理において下記の利用者情報および署名情報はU1, S1であり、代理店が行う暗号化および復号はE3 (), D3 ()である。また、第2の検証処理において下記の利用者情報および署名情報はU2, S2である。なお、ここでは上述の文献[1]、[2]と同様に画像データは透かし情報の変形および消去を受けないという仮定をおく。

【0067】[検証処理]

1) まず第1の検証処理で、第1端末装置10において第1のエンティティは、発見した不正画像Gw' = $G + U' + D1 (S')$ から利用者情報U'を抽出し、さらに上記不正画像Gw'を1次暗号化して署名情報S'を抽出する。ここで利用者情報U'が抽出されない場合は、第1のエンティティの不正と認定する。

【0068】2) 第1の検証処理において正しい署名情報が抽出された場合(S' = Sの場合)は、第2の検証処理へと進む。第2の検証処理においても同様の処理を行い、正しい署名情報が抽出された場合は、第2のエンティティの不正と認定する。これは、正しい署名情報は第2のエンティティにしか作成できず、第1のエンティティは署名情報を知ることにはできないためである。3) また、正しい署名情報が抽出されない場合(S' ≠ Sの場合)は、第1のエンティティの不正と認定する。

【0069】この第1の実施形態による電子透かし方式では、デジタルデータの暗号化処理および電子透かし情報の埋め込み処理を第1端末装置10と第2端末装置20との両方でを行い、暗号処理および埋め込んだ電子透かし情報の正当性の確認を検証局端末装置30が行っているため、第1のエンティティまたは第2のエンティティが単独で不正コピーを行ってもその不正行為を容易に確認することができ、また、不正者も簡単に検証することができる。

【0070】また、この方式では第1の埋込処理および第2の埋込処理の各処理ごとに検証局による検査が行われるので、結託は意味を持たず、サーバまたは原作者と代理店とユーザとの何れかの結託はあり得ない。仮に結託しても、不正行為は容易に確認することができる。なお、この処理の安全性は、検証局が信頼できるということに根拠を置く。

【0071】[第2の実施形態] 近年、電子現金と呼ばれるネットワーク上の通貨が実現されつつある。この電子現金は、通常の現金と同様に所有者の名前が記されな

いので匿名性が実現されている。もし、匿名性が実現されない場合、商品の売り手は、電子現金から誰がどの商品を購入したかという情報を知ることができ、ユーザのプライバシーが犯されることになる。このため、上述した電子透かしによる著作権者の著作権保護と同様に、ユーザのプライバシー保護の実現は重要である。

【0072】そこで、この第2の実施形態では、購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには、電子透かしの本来の目的である不正配布者の特定が行えるようにする。これは、例えば、図2に示すようなシステム200により実現される。このシステム200は、上述した第1の実施形態におけるシステム100と同様の構成としているが、第2端末装置20には、認証局40からの匿名公開鍵証明書が与えられる構成としている。

【0073】通常、署名情報を検査する公開鍵には、その正当性を証明するために認証局と呼ばれる機関による証明書が付されていることが多い。この認証局とは、公開鍵暗号方式におけるユーザの公開鍵の正当性を保証するために、ユーザの公開鍵に証明書を発行する機関を言う。すなわち、認証局は、ユーザの公開鍵やユーザに関するデータに認証局の秘密鍵で署名を施すことによって証明書を作成し、発行する。あるユーザから自分の証明書付き公開鍵を送られた他のユーザは、この証明書を認証局の公開鍵で検査することによって、公開鍵を送ってきたユーザの正当性（少なくとも、認証局によって認められたユーザであるということ）を認証する。このような認証局を運営している組織として、VeriSignやCyberTrustという企業がよく知られている。

【0074】よって、上述した第1の実施形態で述べた第2の埋込処理中の2)の手順において代理店がユーザの契約情報を署名から確認する場合、図2の認証局40の証明書付きの公開鍵で確認することが考えられる。しかしながら、この証明書には通常、公開鍵の所有者の名前が記されている。よってこの場合、データの購入時におけるユーザの匿名性は実現されていないことになる。

【0075】これに対して、公開鍵とその所有者との対応を認証局40が秘密に保持すれば、公開鍵の証明書に所有者の名前を記さないこともできる。このような匿名性を有する公開鍵の証明書を、以後「匿名公開鍵証明書」と呼び、そのような証明書付きの公開鍵を「証明書付き匿名公開鍵」と呼ぶ。そこで、ユーザは、上述した第2の埋込処理中の1)の手順において、契約情報と一緒に契約情報の署名、および署名情報Sを検査するための証明書付き匿名公開鍵を送れば、ユーザはデジタルデータの購入時に自分を匿名にすることができる。

【0076】よって、代理店には利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正コピーの発見時には、その証明書付き匿名公開鍵を認証局40に示してその公開鍵に対応するユーザを教えてもらうこ

とによって、ユーザを特定することができる。以上のことから、上述した第1の実施形態で述べた第2の埋込処理中の1)、2)の手順と、第2の検証処理中の1)の手順とを以下のように変えることにより、ユーザのデジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【0077】以下、上記図2のシステム200における埋め込み処理、および検証処理について具体的に説明する。

【0078】[埋め込み処理]

1) まず、第2端末装置20において、契約生成処理部21は、認証局40で発行された証明書付き匿名公開鍵と一緒に、所望の画像データを要求する契約情報をその公開鍵に対応する署名を付けて第1端末装置10に送る。

2) 次に、第1端末装置10において、契約確認処理部11は、第2のエンティティの公開鍵を認証局40の公開鍵によって検査するとともに、契約情報の署名を第2のエンティティの匿名公開鍵から確認し、その確認後に、少なくとも契約情報および証明書付き匿名公開鍵の一方から利用者情報Uを作成する。そして、電子透かし埋め込み処理部12により上記契約確認処理部11で作成された利用者情報Uを要求された画像データGに埋め込んだ後、1次暗号化処理部13により1次暗号化処理E1()を行い、得られたデータを第2端末装置20に送る。よって、第2端末装置20には、1次暗号化画像データE1(G+U)の情報が送られる。以下の3)～6)の手順は第1の実施形態で述べた手順と同様なので、ここでは重複する説明を省略する。

【0079】[検証処理]

1) 第2の検証処理で第1端末装置10は、発見した不正画像G_{ww'}から利用者情報を抽出し、さらに不正画像G_{ww'}を1次暗号化して署名情報を抽出する。さらに、その抽出された利用者情報と契約情報から分かる匿名公開鍵とを認証局40に示し、その匿名公開鍵に対応する第2のエンティティ名を聞く。ここで利用者情報が抽出されない場合は、第1のエンティティの不正と認定する。以下の2)および3)の手順は第1の実施形態で述べた手順と同様である。

【0080】以上述べたように、第2の実施形態によれば、ユーザはデジタルデータの購入時において検証局に対しても匿名性が保つことができる。

【0081】[第3の実施形態] 第3の実施形態では、図16または図17に示したサーバまたは著作権者が代理店を通してユーザにデジタルデータを配付する処理を一括して考える。以下、本発明に係る第3の実施形態を、図3を参照しながら説明する。すなわち、第3の実施形態に係る電子透かし方式は、例えば、図3に示すようなシステム300により実施され、このシステム300は、本発明に係る電子情報配布システムを適用したも

のでもある。

【0082】第3の実施形態に係るシステム300は、サーバ側の端末装置（以下、サーバ端末装置と記す）50、代理店側の端末装置（以下、代理店端末装置と記す）60、ユーザ側の端末装置（以下、ユーザ端末装置と記す）70および検証局側の端末装置（以下、検証局端末装置と記す）30を含む多数のエンティティ（図示せず）からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにデジタルデータの授受を行うようになされている。

【0083】サーバ端末装置50は、例えば画像データ（デジタルデータ）が供給される1次暗号化処理部51と、ユーザ端末装置70および検証局端末装置30からのデータが供給される1次復号処理部52とを備えており、1次暗号化処理部51の出力が代理店端末装置60に送信されるとともに、1次復号処理部52の出力がユーザ端末装置70に送信されるようになされている。

【0084】代理店端末装置60は、ユーザ端末装置70からのデータが供給される契約確認処理部61と、サーバ端末装置50の1次暗号化処理部51の出力が供給される電子透かし埋め込み処理部62とを備えており、電子透かし埋め込み処理部62の出力がユーザ端末装置70および検証局端末装置30に送信されるようになされている。

【0085】ユーザ端末装置70は、代理店端末装置60の契約確認処理部61に対してデータを送信する契約生成処理部71と、署名生成処理部72と、署名生成処理部72および代理店端末装置60の電子透かし埋め込み処理部62からのデータが供給される電子透かし埋め込み処理部73と、電子透かし埋め込み処理部73の出力が供給される2次暗号化処理部74と、サーバ端末装置50の1次復号処理部52からのデータが供給される2次復号処理部75とを備えており、2次復号処理部75の出力が電子透かし付き画像データとして出力されるようになされている。また、2次暗号化処理部74の出力は、サーバ端末装置50の1次復号処理部52および検証局端末装置30に各々供給されるようになされている。

【0086】検証局端末装置30は、代理店端末装置60の電子透かし埋め込み処理部62およびユーザ端末装置70の2次暗号化処理部74の出力が供給される2次復号処理部31と、2次復号処理部31の出力が供給される電子透かし確認処理部32とを備えており、電子透かし確認処理部32の出力がサーバ端末装置50の1次復号処理部52に供給されるようになされている。

【0087】以下に、上記のように構成したシステム300の動作を説明する。なお、この図3に示されるプロトコルにおいて、方式や秘密鍵等の1次暗号に関する情報はサーバまたは著作者だけが知る情報であり、2次暗号に関する情報はユーザだけが知る情報である。ただ

し、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下では、図17のような階層システムを対象にして説明を行うが、以下において著作者をサーバと読み替えれば、図16のシステムに対する説明となる。

【0088】[埋め込み処理]

1) まず、ユーザ端末装置70において、ユーザが署名を付けて代理店端末装置60に所望の画像データを要求する。この要求データは、契約生成処理部71により生成された情報（ユーザの署名情報）であり、以下ではこれを契約情報と呼ぶ。代理店では、契約確認処理部61において、受信した契約情報をユーザの署名から確認し、その確認後に画像データをサーバ端末装置50（著作者）に要求する。これを受けてサーバ端末装置50における1次暗号化処理部51は、画像データGに対して1次暗号化処理E1（）を行い、得られたデータE1（G）を代理店端末装置60に送る。

【0089】2) 次に、代理店端末装置60において、契約確認処理部61は、ユーザ端末装置70より受信した契約情報から利用者情報Uを作成する。そして、電子透かし埋め込み処理部62は、上記契約確認処理部61で作成された利用者情報Uをサーバ端末装置50から送られた1次暗号化画像データE1（G）に埋め込み、ユーザ端末装置70に送る。よって、ユーザ端末装置70には、利用者情報付きの1次暗号化画像データE1（G）+Uの情報が送られることになる。

【0090】このとき、代理店端末装置60の電子透かし埋め込み処理部62は、電子透かしに関する秘密情報を検証局端末装置30に送る。なお、秘密情報とは、電子透かしを検出するための埋め込み位置や強度に関する情報であり、検証局端末装置30と共有している他の暗号方式によって暗号化して送られるものである。

【0091】3) 次に、ユーザ端末装置70において、署名生成処理部72は、自分の秘密鍵を用いて署名情報Sを生成する。そして、電子透かし埋め込み処理部73は、署名生成処理部72で生成された署名情報Sを、代理店端末装置60から送られてきた（配布された）1次暗号化画像データE1（G）+Uに埋め込む。また、2次暗号化処理部74は、電子透かし埋め込み処理部73で署名情報Sが埋め込まれた1次暗号化画像データE1（G）+U+Sを2次暗号化して検証局端末装置30に送る。よって、検証局端末装置30には、2次暗号化画像データE2（E1（G）+U+S）の情報が送られることになる。

【0092】このとき、ユーザ端末装置70の2次暗号化処理部74は、検証局端末装置30への送信データ（2次暗号化画像データE2（E1（G）+U+S））に対するハッシュ値H2を生成および署名し、電子透かしに関連する秘密情報と、2次暗号化の秘密鍵とを共に

検証局端末装置30に送る。

【0093】4) 次に、検証局端末装置30では、ユーザ端末装置70から送られてきたハッシュ値H2の署名と、そのハッシュ値H2が送信データのハッシュ値と一致することを確認し、その確認後に2次復号処理部31は、ユーザ端末装置70からの2次暗号化画像データE2 (E1 (G) + U + S) を復号し、そこから利用者情報Uと署名情報Sとを抽出する。そして、電子透かし確認処理部32で上記利用者情報Uと署名情報Sとを検査し、正しければ検証情報を作成して検証局端末装置30の署名を付ける。最後に、検証局端末装置30は、ユーザ端末装置70から送信された2次暗号化画像データE2 (E1 (G) + U + S) とハッシュ値H2とその署名、およびそれに対する検証情報とその署名とをサーバ端末装置50に送る。

【0094】5) 次に、サーバ端末装置50において、著作者は、検証局端末装置30から送られてきた検証情報とその署名とを確認し、さらに2次暗号化画像データE2 (E1 (G) + U + S) とハッシュ値H2とその署名とを確認する。その確認後に1次復号処理部52は、上記2次暗号化画像データE2 (E1 (G) + U + S) の1次暗号化を復号してE2 (G) + D1 (E2 (U + S)) の情報を生成し、それをユーザ端末装置70に送る。

【0095】6) 次に、ユーザ端末装置70において、2次復号処理部75は、サーバ端末装置50から送られてきたE2 (G) + D1 (E2 (U + S)) の情報の2次暗号化を復号して電子透かし付き画像データGwを取り出す。よって、電子透かし付き画像データGwは、 $Gw = G + D1 (U + S)$ と表わされる。これは、もとの画像データGに対して1次復号の影響を受けた利用者情報Uとユーザの署名情報Sとが透かし情報として埋め込まれていることを示す。

【0096】もし、著作者またはユーザのどちらかの不正によって上記4) の過程において正しい透かし情報が検証局端末装置30で検証されない場合、そのことがサーバ端末装置50と代理店端末装置60とユーザ端末装置70とに知らせられる。この時点で取り引きが中止されても、誰にとっても利益も不利益もなく、不正をする意味がない。なお、不正コピー (不正画像) Gw' が発見された場合は、以下のような簡単な検証処理で不正者を容易に特定できる。ただし、ここでは上述の文献[1]、[2]と同様に、画像データは透かし情報の変形および消去を受けないという仮定をおく。

【0097】[検証処理]

1) まず、サーバ端末装置50において、著作者は発見した不正画像Gw' を1次暗号化して利用者情報を抽出する。ここで利用者情報が抽出されない場合は著作者の不正と認定する。

2) 一方、正しい利用者情報が抽出された場合は、上記

不正画像Gw' を1次暗号化したデータから署名情報を抽出する。

3) ここで、正しい署名情報が抽出された場合は、ユーザの不正と認定する。これは、正しい署名情報はユーザにしか作成できず、著作者および代理店は署名情報を知ることとはできないためである。

4) また、正しい署名情報が抽出されない場合は著作者の不正と認定する。

【0098】この第3の実施形態による電子透かし方式では、デジタルデータの暗号化処理および電子透かし情報の埋め込み処理をサーバ端末装置50と代理店端末装置60とユーザ端末装置70との三者で行い、暗号化処理および埋め込んだ電子透かし情報の正当性の確認を検証局端末装置30が行っているため、著作者、代理店またはユーザが単独で不正コピーを行ってもその不正行為を容易に確認することができ、また、不正者も簡単に検証することができる。また、この方式では著作者、代理店およびユーザの利害は相反するので結託はあり得ない。仮に結託しても、不正行為は容易に確認することができる。なお、この処理の安全性は、検証局が信頼できるということに根拠を置く。

【0099】[第4の実施形態] 第4の実施形態においても第3の実施形態と同様に、図16または図17に示したサーバまたは著作者が代理店を通してユーザにデジタルデータを渡す処理を一括して考える。以下、本発明に係る第4の実施形態を、図4を参照しながら説明する。すなわち、第4の実施形態に係る電子透かし方式は、例えば、図4に示すようなシステム400により実施され、このシステム400は、本発明に係る電子情報配布システムを適用したものでもある。

【0100】第4の実施形態に係るシステム400は、サーバ端末装置50、代理店端末装置60、ユーザ端末装置70および検証局端末装置30を含む多数のエンティティ (図示せず) からなるネットワークシステムであり、各エンティティは、ネットワークを介して互いにデジタルデータの授受を行うようになされている。

【0101】サーバ端末装置50は、例えば画像データ (デジタルデータ) が供給される1次暗号化処理部51と、代理店端末装置60および検証局端末装置30からのデータが供給される1次復号処理部52とを備えており、1次暗号化処理部51の出力が代理店端末装置60に送信されるとともに、1次復号処理部52の出力がユーザ端末装置70に送信されるようになされている。

【0102】代理店端末装置60は、ユーザ端末装置70からのデータが供給される契約確認処理部61と、契約確認処理部61およびサーバ端末装置50の1次暗号化処理部51の出力が供給される電子透かし埋め込み処理部62と、ユーザ端末装置70からのデータが供給される電子透かし埋め込み処理部63とを備えており、一方の電子透かし埋め込み処理部62の出力がユーザ端末

装置 70 に送信されるとともに、他方の電子透かし埋め込み処理部 63 の出力がサーバ端末装置 50 および検証局端末装置 30 に送信されるようになされている。

【0103】ユーザ端末装置 70 は、代理店端末装置 60 の契約確認処理部 61 に対してデータを送信する契約生成処理部 71 と、署名生成処理部 72 と、代理店端末装置 60 の電子透かし埋め込み処理部 62 の出力が供給される 2 次暗号化処理部 74 と、サーバ端末装置 50 の 1 次復号処理部 52 からのデータが供給される 2 次復号処理部 75 とを備えており、2 次復号処理部 75 の出力が電子透かし付き画像データとして出力されるようになされている。また、2 次暗号化処理部 74 の出力は、代理店端末装置 60 の電子透かし埋め込み処理部 63 および検証局端末装置 30 に各々供給されるようになされている。

【0104】検証局端末装置 30 は、代理店端末装置 60 の電子透かし埋め込み処理部 63 およびユーザ端末装置 70 の 2 次暗号化処理部 74 の出力が供給される 2 次復号処理部 31 と、2 次復号処理部 31 および代理店端末装置 60 の電子透かし埋め込み処理部 63 の出力が供給される電子透かし確認処理部 32 とを備えており、電子透かし確認処理部 32 の出力がサーバ端末装置 50 の 1 次復号処理部 52 に供給されるようになされている。

【0105】以下に、上記のように構成したシステム 400 の動作を説明する。なお、この図 4 に示されるプロトコルにおいて、方式や秘密鍵等の 1 次暗号に関する情報はサーバまたは著作者だけが知る情報であり、2 次暗号に関する情報はユーザだけが知る情報である。ただし、これらの暗号の間には、どちらの暗号化を先に行っても復号を行うとその暗号は解かれる、という性質を持つものとする。以下では、図 17 のような階層システムを対象にして説明を行うが、以下において著作者をサーバと読み替えれば、図 16 のシステムに対する説明となる。

【0106】[埋め込み処理]

1) まず、ユーザ端末装置 70 において、ユーザが署名を付けて代理店端末装置 60 に所望の画像データを要求する。この要求データは、契約生成処理部 71 により生成された情報（ユーザの署名情報）であり、以下ではこれを契約情報と呼ぶ。代理店では、契約確認処理部 61 において、受信した契約情報をユーザの署名から確認し、その確認後に画像データをサーバ端末装置 50（著作者）に要求する。これを受けてサーバ端末装置 50 における 1 次暗号化処理部 51 は、画像データ G に対して 1 次暗号化処理 E1 () を行い、得られたデータ E1 (G) を代理店端末装置 60 に送る。

【0107】2) 次に、代理店端末装置 60 において、契約確認処理部 61 は、ユーザ端末装置 70 より受信した契約情報から利用者情報 U を作成する。そして、電子透かし埋め込み処理部 62 は、上記契約確認処理部 61

で作成された利用者情報 U をサーバ端末装置 50 から送られた 1 次暗号化画像データ E1 (G) に埋め込み、ユーザ端末装置 70 に送る。よって、ユーザ端末装置 70 には、利用者情報付きの 1 次暗号化画像データ E1 (G) + U の情報が送られることになる。

【0108】3) 次に、ユーザ端末装置 70 において、2 次暗号化処理部 74 は、代理店端末装置 60 より送られた 1 次暗号化画像データ E1 (G) + U を 2 次暗号化し、得られた画像データ E2 (E1 (G) + U) の情報を代理店端末装置 60 に送る。このとき、署名生成処理部 72 では、ユーザが自分にしか作成できない署名情報 S を生成し、2 次暗号化画像データ E2 (E1 (G) + U) と共に代理店端末装置 60 に送る。また、2 次暗号化処理部 74 は、2 次暗号化の秘密鍵を検証局端末装置 30 に送る。

【0109】4) 次に、代理店端末装置 60 において、電子透かし埋め込み処理部 63 は、ユーザ端末装置 70 から送られてきた 2 次暗号化画像データ E2 (E1 (G) + U) に対して同じくユーザ端末装置 70 から送られてきた署名情報 S を埋め込み、検証局端末装置 30 に送る。よって、検証局端末装置 30 には、署名情報付きの 2 次暗号化画像データ E2 (E1 (G) + U) + S の情報が送られることになる。

【0110】このとき、代理店端末装置 60 では、検証局端末装置 30 への送信データ（2 次暗号化画像データ E2 (E1 (G) + U) + S）に対するハッシュ値 H2 を生成および署名し、電子透かしに関連する秘密情報と共に検証局端末装置 30 に送る。なお、秘密情報とは、電子透かしを検出するための埋め込み位置や強度に関する情報であり、検証局端末装置 30 と共有している他の暗号方式によって暗号化して送られるものである。

【0111】5) 次に、検証局端末装置 30 では、代理店端末装置 60 から送られてきたハッシュ値 H2 の署名と、そのハッシュ値 H2 が送信データのハッシュ値と一致することを確認し、その確認後に、電子透かし確認処理部 32 で代理店端末装置 60 からの 2 次暗号化画像データ E2 (E1 (G) + U) + S より署名情報 S を抽出するとともに、2 次復号処理部 31 で上記 2 次暗号化画像データ E2 (E1 (G) + U) + S の 2 次暗号化を復号し、そこから利用者情報 U を抽出する。

【0112】そして、電子透かし確認処理部 32 は、上記抽出した利用者情報 U と署名情報 S とを検査し、正しければ検証情報を作成して検証局端末装置 30 の署名を付ける。最後に、検証局端末装置 30 は、代理店端末装置 60 から送信された 2 次暗号化画像データ E2 (E1 (G) + U) + S とハッシュ値 H2 とその署名、およびそれに対する検証情報とその署名とをサーバ端末装置 50 に送る。

【0113】6) 次に、サーバ端末装置 50 において、著作者は、検証局端末装置 30 から送られてきた検証情

報とその署名とを確認し、さらに2次暗号化画像データE2(E1(G)+U)+Sとハッシュ値H2とその署名とを確認する。その確認後に1次復号処理部52は、上記2次暗号化画像データE2(E1(G)+U)+Sの1次暗号化を復号してE2(G)+D1(E2(U)+S)の情報を生成し、それをユーザ端末装置70に送る。

【0114】7) 次に、ユーザ端末装置70において、2次復号処理部75は、サーバ端末装置50から送られてきたE2(G)+D1(E2(U)+S)の情報の2次暗号化を復号して電子透かし付き画像データGwを取り出す。よって、電子透かし付き画像データGwは、 $Gw = G + D1(U + D2(S))$ と表わされる。これは、もとの画像データGに対して1次復号の影響を受けた利用者情報Uと更に2次復号の影響も受けた署名情報Sとが透かし情報として埋め込まれていることを示す。

【0115】もし、著作者またはユーザのどちらかの不正によって上記5)の過程において正しい透かし情報が検証局端末装置30で検証されない場合、そのことがサーバ端末装置50と代理店端末装置60とユーザ端末装置70とに知らせられる。この時点で取り引きが中止されても、誰にとっても利益も不利益もなく、不正をする意味がない。なお、不正コピー(不正画像)Gw'が発見された場合は、以下のような簡単な検証処理で不正者を容易に特定できる。ただし、ここでは上述の文献[1]、[2]と同様に、画像データは透かし情報の変形および消去を受けないという仮定をおく。

【0116】[検証処理]

1) まず、サーバ端末装置50において、著作者は発見した不正画像Gw'を1次暗号化して利用者情報U'を抽出する。ここで利用者情報U'が抽出されない場合は著作者の不正と認定する。

2) 一方、正しい利用者情報が抽出された場合、サーバ端末装置50は、1次暗号化された画像データGw'と利用者情報U'とを検証局端末装置30に示し、検査を要求する。検証局端末装置30は、1次暗号された画像データGw'を2次暗号化し(この暗号化機能は不図示)、署名情報を抽出する。

3) ここで、正しい署名情報が抽出された場合はユーザの不正と認定する。

4) また、正しい署名情報が抽出されない場合は著作者の不正と認定する。

【0117】この第4の実施形態による電子透かし方式でも、デジタルデータの暗号化処理および電子透かし情報の埋め込み処理をサーバ端末装置50と代理店端末装置60とユーザ端末装置70との三者で行い、暗号処理および埋め込んだ電子透かし情報の正当性の確認を検証局端末装置30が行っているため、著作者、代理店またはユーザが単独で不正コピーを行ってもその不正行為を容易に確認することができ、また、不正者も簡単に検

証することができる。また、この方式では著作者、代理店およびユーザの利害は相反するので結託はあり得ない。仮に結託しても、不正行為は容易に確認することができる。なお、この処理の安全性は、検証局が信頼できるということに根拠を置く。

【0118】[第5の実施形態] 第5の実施形態は、図3に示した第3の実施形態において、第2の実施形態と同様にデジタルデータの購入時にはユーザの匿名性が実現され、画像の不正配布のような不正が発見されたときには不正配布者の特定が行えるようにしたものである。これは、例えば、図5に示すようなシステム500により実現される。このシステム500は、上述した第3の実施形態におけるシステム300と同様の構成としているが、ユーザ端末装置70には、認証局40からの匿名公開鍵証明書が与えられる構成としている。

【0119】本実施形態でも第2の実施形態と同様に、公開鍵とその所有者との対応を認証局40が秘密に保持することにより、公開鍵の証明書に所有者の名前を記さないことができるようにしている。そこで、ユーザは、上述した第3の実施形態における埋め込み処理中の1)の手順において、契約情報と一緒に契約情報の署名、および署名情報Sを検査するための証明書付き匿名公開鍵を送れば、ユーザはデジタルデータの購入時に自分を匿名にすることができる。

【0120】よって、代理店には利用者を特定する情報として証明書付き匿名公開鍵が渡されるが、不正コピーの発見時には、その証明書付き匿名公開鍵を認証局40に示してその公開鍵に対応するユーザを教えてもらうことによって、ユーザを特定することができる。以上のことから、上述した第3の実施形態で述べた埋め込み処理中の1)の手順と、検証処理中の1)の手順とを以下のように変えることにより、ユーザのデジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【0121】なお、第4の実施形態を示す図4のシステム400中のユーザ端末装置70に対して認証局40を設け、上述した第4の実施形態で述べた埋め込み処理中の1)の手順と、検証処理中の1)の手順とを以下のように変えることによっても、ユーザのデジタルデータ購入時の匿名性と不正発見時の不正者特定との両方を実現することができる。

【0122】以下、上記図5のシステム500における埋め込み処理、および検証処理について具体的に説明する。

【0123】[埋め込み処理]

1) まず、ユーザ端末装置70において、契約生成処理部71は、認証局40で発行された証明書付き匿名公開鍵と一緒に、所望の画像データを要求する契約情報をその公開鍵に対応する署名を付けて代理店端末装置60に送る。代理店では、契約確認処理部61において、受信

した契約情報を匿名公開鍵から確認し、その確認後に画像データを著作者に要求する。これを受けてサーバ端末装置50における1次暗号化処理部51は、画像データGに対して1次暗号化処理E1()を行い、得られたデータE1(G)を代理店端末装置60に送る。以下の2)～6)の手順は第3の実施形態で述べた手順と同様なので、ここでは重複する説明を省略する。

【0124】[検証処理]

1) サーバ端末装置50において1次暗号各処理部51は、発見した不正画像G'を1次暗号化して利用者情報を抽出する。そして、その抽出した利用者情報と契約情報から分かる匿名公開鍵とを認証局40に示し、その匿名公開鍵に対応するユーザ名を聞く。ここで利用者情報が抽出されない場合は、著作者の不正と認定する。以下の2)～4)の手順は第3の実施形態で述べた手順と同様である。

【0125】以上述べたように、第5の実施形態によれば、ユーザはデジタルデータの購入時において検証局に対しても匿名性が保つことができる。

【0126】上述の第1～第5の実施形態に示した画像データ、および電子透かし情報の埋め込み処理によって得られるハッシュ値を含む種々のデータは、以下のような画像フォーマットで格納することができる。例えば、下記の一般的な画像フォーマットでは、各段階で送付される画像データを画像データ部に格納し、それに対応するハッシュ値やその署名などを画像ヘッダ部に格納することができる。また、最終的にユーザが保存しておく必要があるハッシュ値およびその署名や、2次暗号の鍵等を画像ヘッダ部に、電子透かし付き画像データを画像データ部に格納しておくことができる。

【0127】一方、下記に示すFlashPixTMファイルフォーマットでは、上記のようなハッシュ値やその署名を含む一般的な画像フォーマットを各階層のデータとして格納することができる。また、ハッシュ値やその署名などは、属性情報としてプロパティセットの中に格納しておくこともできる。

【0128】まず、一般的な画像フォーマットについて説明する。一般的な画像フォーマットでは、図6に示すように、画像ファイルは画像ヘッダ部と画像データ部とに分けられる。

【0129】一般的に画像ヘッダ部には、その画像ファイルから画像データを読み取る時に必要な情報や、画像の内容を説明する付帯的な情報が格納される。図6の例では、その画像フォーマット名を示す画像フォーマット識別子、ファイルサイズ、画像の幅・高さ・深さ、圧縮の有無、解像度、画像データの格納位置へのオフセット、カラーパレットのサイズなどの情報が格納されている。一方、画像データ部は、画像データを順次格納している部分である。このような画像フォーマットの代表的な例としては、Microsoft社のBMPフォーマットやCo

mpuserve社のGIFフォーマットなどが広く普及している。

【0130】次に、FlashPixTMファイルフォーマットについて具体的に説明する。以後説明するFlashPixTM(FlashPixは米国Eastman Kodak社の登録商標)ファイルフォーマットでは、上記画像ヘッダ部に格納されていた画像属性情報および画像データ部に格納されていた画像データを、更に構造化してファイル内に格納する。この構造化した画像ファイルを、図7および図8に示す。ファイル内の各プロパティやデータには、MS-DOSのディレクトリとファイルに相当する、ストレージとストリームによってアクセスする。上記図7、図8において、影付き部分がストレージで、影なし部分がストリームである。画像データや画像属性情報はストリーム部分に格納される。

【0131】図7において、画像データは異なる解像度で階層化されており、それぞれの解像度の画像をSubimageと呼び、Resolution 0, 1, ..., nで示してある。各解像度の画像に対して、その画像データを読み出すために必要な情報がSubimage Headerに、また画像データがSubimage dataに格納される。プロパティセットとは、属性情報をその使用目的や内容に応じて分類して定義したものであり、Summary info. Property Set、Image info. Property Set、Image Content Property Set、Extension list property Setがある。

【0132】[各プロパティセットの説明]Summary info. Property Setは、FlashPix特有のものではなく、Microsoft社のストラクチャードストレージでは必須のプロパティセットで、そのファイルのタイトル・題名・著者・サムネール画像等を格納する。また、Comp Obj. Streamには記憶部(Strage)に関する一般的な情報が格納される。

【0133】Image Content Property Setは、画像データの格納方法を記述する属性である(図9参照)。この属性には、画像データの階層数、最大解像度の画像の幅や高さ、それぞれの解像度の画像についての幅、高さ、色の構成、あるいはJPEG圧縮を用いる際の量子化テーブル・ハフマンテーブルの定義などを記述する。Extension list property Setは、上記FlashPixの基本仕様

に含まれない情報を追加する際に使用する領域である。さらに、ICC Profileの部分には、ICC(International Color Consortium)において規定される色空間変換のための変換プロファイルが記述される。

【0134】また、Image info. Property Setは、画像データを使用する際に利用できる様々な情報、例えば、その画像がどのようにして取り込まれ、どのように利用可能であるかの下記のような情報を格納する。

・デジタルデータの取り込み方法/あるいは生成方法に関する情報

・著作権に関する情報

- ・画像の内容（画像中の人物、場所など）に関する情報
- ・撮影に使われたカメラに関する情報
- ・撮影時のカメラのセッティング（露出、シャッタースピード、焦点距離、フラッシュ使用の有無など）の情報
- ・デジタルカメラ特有の解像度やモザイクフィルタに関する情報
- ・フィルムのメーカー名、製品名、種類（ネガ／ポジ、カラー／白黒）等の情報
- ・オリジナルが書物や印刷物である場合の種類やサイズに関する情報
- ・スキャン画像の場合、使用したスキャナやソフト、操作した人に関する情報

【0135】図8のFlashPix Image View Objectは、画像を表示する際に用いるビューイングパラメータと画像データとを合わせて格納する画像ファイルである。ビューイングパラメータとは、画像の回転、拡大／縮小、移動、色変換、フィルタリングの処理を画像表示の際に適応するために記憶しておく処理係数のセットである。この図8において、Global info. Property Setの部分には、ロックされている属性リストが記述されており、例えば、最大画像のインデックスや最大変更項目のインデックス、最終修正者の情報などが記述される。

【0136】また、同図において、Source/Result FlashPix Image Object は、FlashPix画像データの実体であり、Source FlashPix Image Objectは必須で、Result FlashPix Image Objectはオプションである。Source FlashPix Image Objectはオリジナルの画像データを、Result FlashPix Image Objectはビューイングパラメータを使って画像処理した結果の画像データをそれぞれ格納する。

【0137】また、Source/Result desc. Property Setは、上記画像データの識別のためのプロパティセットであり、画像ID、変更禁止のプロパティセット、最終更新日時等を格納する。Transform Property Setは、画像の回転、拡大／縮小、移動のためのAffine変換係数、色変換マトリクス、コントラスト調整値、フィルタリング係数を格納している。

【0138】次に、画像データの取り扱いについて説明する。ここでは、複数のタイルに分割された複数の解像度の画像を含む画像フォーマットを例に挙げて説明する。図10に、解像度の異なる複数の画像から構成される画像ファイルの例を示す。この図10において、最大解像度の画像は列×行が $X0 \times Y0$ で構成されており、その次に解像度の大きい画像は $X0/2 \times Y0/2$ であり、それ以降順次、列・行ともに $1/2$ ずつ縮小し、列・行ともに64画素以下あるいは互いに等しくなるまで縮小されていく。

【0139】このように画像データを階層化した結果、画像の属性情報として「1つの画像ファイル中の階層数」や、それぞれの階層の画像に対して、一般的な画像

フォーマットの項で説明したヘッダ情報と画像データとが必要となる（図6参照）。1つの画像ファイル中の階層の数や最大解像度の画像の幅、高さ、あるいはそれぞれの解像度の画像の幅、高さ、色構成、圧縮方式等に関する情報は、上記ImageContent Property Set中に記述される（図9参照）。

【0140】さらに、各解像度のレイヤの画像は、図11に示すように64画素×64画素でなるタイル毎に分割されている。画像の左上部から順次64画素×64画素のタイルに分割をすると、画像によっては右端および下端のタイルの一部に空白が生ずる場合がある。この場合は、それぞれ最右端画像または最下端画像を繰り返し挿入することで、64画素×64画素を構築する。

【0141】FlashPixTMでは、それぞれのタイル中の画像データをJPEG圧縮、シングルカラー、非圧縮のいずれかの方法で格納する。JPEG圧縮は、ISO/IEC JTC1/SC29により国際標準化された画像圧縮方式であり、方式自体の説明はここでは割愛する。また、シングルカラーとは、上記1つのタイルがすべて同じ色で構成されている場合にのみ、個々の画素の値を記録することなく、そのタイルの色を1色で表現する方式である。この方法は特に、コンピュータグラフィックスにより生成された画像で有効である。

【0142】このようにタイル分割された画像データは、例えば図7のSubimage data ストリーム中に格納され、タイルの総数、個々のタイルのサイズ、データの開始位置、圧縮方法はすべてSubimage Header に格納されている（図12参照）。

【0143】〔その他の実施形態〕以上に述べた第1～第5の実施形態において、透かし情報の埋め込みは、種々の手法によって実現できるが、例えば、「清水，沼尾，森本（日本IBM）：「ピクセルブロックによる静止画像データハイディング」，情報処理学会第53回全国大会，1N-11，平成8年9月」の文献や、「I. J. Cox, J. Kilian, T. Leighton and T. Shamoon (NEC) : "Secure Spread Spectrum Watermarking for Multimedia," NEC Research Institute Technical Report 95-10.」の文献に示されるような公知の埋め込み手法によって実現できる。

【0144】また、1次暗号，2次暗号として用いられる暗号方式も種々の方式によって実現できるが、例えばビットの配置を暗号鍵に応じて換えるといった暗号方式によって実現できる。また、全ての送信データにハッシュ値とその署名を付けて送ることもできる。さらに、1次暗号と2次暗号は、透かし情報の埋め込み処理において互いの情報を知らせないために用いられるが、第三者からの通信路上での盗聴および改ざんを防ぐために、別にDES (Data Encryption Standard) 等の暗号やハッシュ関数等を用いても良い。

【0145】また、上述の第1～第5の実施形態におい

て、不正配布の検出は第1のエンティティ（サーバまたは著作者）が行っているが、1次暗号または2次暗号に関する秘密鍵を知らなくても電子透かしの抽出手段さえ持っていれば、誰にでも不正配布および不正配布の利用者情報を知ることができる。その後、不正配布発見を第1のエンティティ側に知らせて検証処理を始めさせれば良いので、不正配布の発見者は第1のエンティティに限定されない。

【0146】また、第1のエンティティまたは代理店は、利用者情報Uだけでなく、必要に応じて著作権情報やその画像データの配布状況に関する情報等の他の情報を画像データに埋め込むこともできる。また、第1のエンティティで秘密の情報を埋め込みたい場合は、1次暗号化の後に埋め込み処理を行えば、署名情報と同様に1次暗号の影響を受けた情報を埋め込むことができる。さらに、利用者情報Uは、必ず1次暗号化の前にある必要はなく、1次暗号化の後に埋め込んでよい（この場合、利用者情報Uの検出は、第1のエンティティまたは1次暗号の秘密鍵を知る者のみが行える）。

【0147】また、第2のエンティティが共通のプリンタや端末等を用いるユーザである場合、第2のエンティティの署名情報および2次暗号は、プリンタや共通端末の署名情報や暗号方式を含む場合がある。また、第1のエンティティからの1次暗号化情報は、第2のエンティティからの契約情報による依頼がなくとも、ネットワークやCD-ROM等によって広く配布されていても良い。また、第2のエンティティの署名情報Sは、公開鍵暗号方式によって生成されなくとも良く、ユーザが契約情報等で定めた情報（暗証番号のような情報）等でも良い。

【0148】また、米国では40ビット以上の暗号を用いる場合、暗号の悪用を防ぐために暗号鍵を管理する鍵管理局を必要とする。そこで、検証局に鍵管理局を兼ねさせることも可能である。よって、検証局が2次暗号の鍵をあらかじめ管理している場合には、不正画像の監視も検証局が行えば、上述の検証処理1)～3)は検証局が単独で行うことができる。第1のエンティティの1次暗号の鍵は、同じ検証局によって管理されていてもよいし、他の鍵管理局によって管理されていてもよい。また、第1のエンティティや第2のエンティティの鍵は、鍵管理局が生成して配布してもよい。

【0149】また、代理店は1つであるとは限らず、階層的に構成されていても良い。このとき、代理店の行う処理は階層中の担当代理店が代表して行っても良いし、代理店間で上記のプロトコルを行い、責任を明らかにするようにしても良い。また、図17のように代理店が1つの場合は、代理店に関する利用者情報U1の埋め込みを省略することができる。

【0150】また、著作者は要求された後に画像データGの1次暗号情報E1(G)を代理店に送ることになっ

ているが、1次暗号化画像データE1(G)をあらかじめ代理店に送るようにしても良い。また、第3の実施形態以降の代理店は暗号E3()および復号D3()を持たないが、著作者から最初にデータを送られた後、暗号E3()によって暗号化し、最後に著作者にデータを送る前に復号D3()によって復号しても良い。

【0151】

【発明の効果】上述の説明から明らかなように、本発明の電子透かし方式および電子情報配布システムによれば、データに対する暗号処理および電子透かし埋め込み処理を複数の手段またはエンティティで分散して行い、上記複数の手段またはエンティティで行われた上記暗号処理および電子透かし埋め込み処理の少なくとも一方の正当性を、上記複数の手段またはエンティティとは別の手段またはエンティティで検証するようにしたので、階層的に構成されたネットワークにおいてデータを不正にコピーして配布を行った際にその不正行為および不正行為者を確実に認識することができ、これによって不正を確実に防止することが可能となり、データの不正配布に関して安全なシステムを実現することができる。さらに、このシステムによってユーザの匿名性や暗号の悪用を防ぐ鍵管理局への応用も容易に実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態を示した電子透かしシステムを説明するための図である。

【図2】本発明の第2の実施形態を示した電子透かしシステムを説明するための図である。

【図3】本発明の第3の実施形態を示した電子透かしシステムを説明するための図である。

【図4】本発明の第4の実施形態を示した電子透かしシステムを説明するための図である。

【図5】本発明の第5の実施形態を示した電子透かしシステムを説明するための図である。

【図6】一般的な画像フォーマットを示す図である。

【図7】FlashPixTMファイルフォーマットの例を示す図である。

【図8】FlashPixTMファイルフォーマットの例を示す図である。

【図9】FlashPixTMファイルフォーマットのImage Content Property Setに格納される属性情報を示す図である。

【図10】それぞれ解像度の異なる複数の画像から構成される画像ファイルの例を示す図である。

【図11】各解像度のレイヤの画像のタイル分割の様子を示す図である。

【図12】タイル分割された画像データに関する属性情報を示す図である。

【図13】従来の電子透かしシステムを説明するための図である。

【図 1 4】図 1 3 に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【図 1 5】図 1 4 に示す方式を改良した従来の電子透かしシステムを説明するための図である。

【図 1 6】階層的に構成されたデータ配付システムの一例を示す図である。

【図 1 7】階層的に構成されたデータ配付システムの他の例を示す図である。

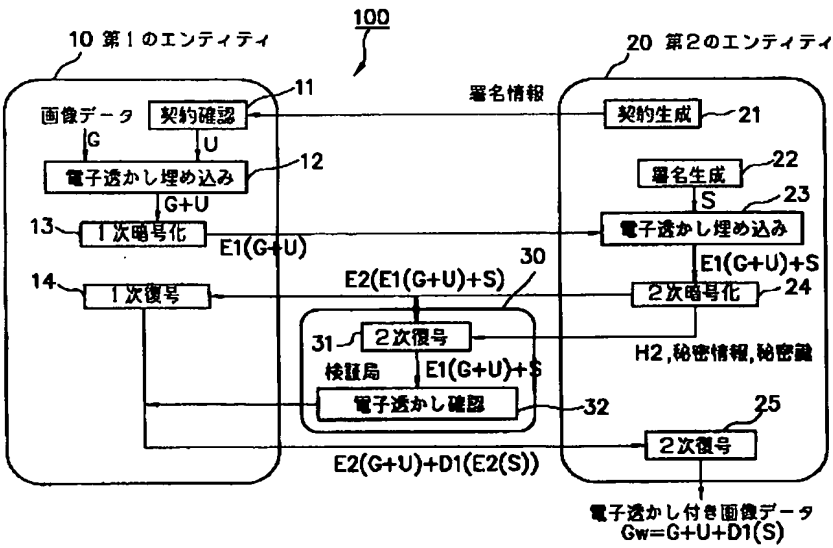
【符号の説明】

- 1 0 第 1 のエンティティ側の端末装置
- 1 1 契約確認処理部
- 1 2 電子透かし埋め込み処理部
- 1 3 1 次暗号化処理部
- 1 4 1 次復号処理部
- 2 0 第 2 のエンティティ側の端末装置
- 2 1 契約生成処理部
- 2 2 署名生成処理部
- 2 3 電子透かし埋め込み処理部
- 2 4 2 次暗号化処理部
- 2 5 2 次復号処理部
- 3 0 検証局端末装置

- * 3 1 2 次復号処理部
- 3 2 電子透かし確認処理部
- 4 0 認証局端末装置
- 5 0 サーバ端末装置
- 5 1 1 次暗号化処理部
- 5 2 1 次復号処理部
- 6 0 代理店端末装置
- 6 1 契約生成処理部
- 6 2 電子透かし埋め込み処理部
- 10 6 3 電子透かし埋め込み処理部
- 7 0 ユーザ端末装置
- 7 1 契約生成処理部
- 7 2 署名生成処理部
- 7 3 電子透かし埋め込み処理部
- 7 4 2 次暗号化処理部
- 7 5 2 次復号処理部
- 1 0 0 電子情報配布システム
- 2 0 0 電子情報配布システム
- 3 0 0 電子情報配布システム
- 20 4 0 0 電子情報配布システム
- * 5 0 0 電子情報配布システム

【図 1】

【図 6】

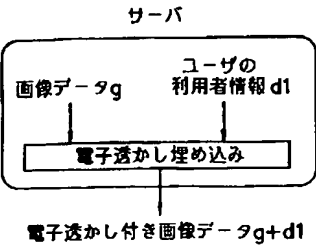


画像ヘッダ部	画像フォーマット識別子
	ファイルサイズ
	X方向ピクセル数(幅)
	Y方向ピクセル数(高さ)
	深さ方向サイズ
	圧縮の有無
	解像度
	ビットマップへのオフセット
画像データ部	カラーパレットサイズ
	ビットマップ

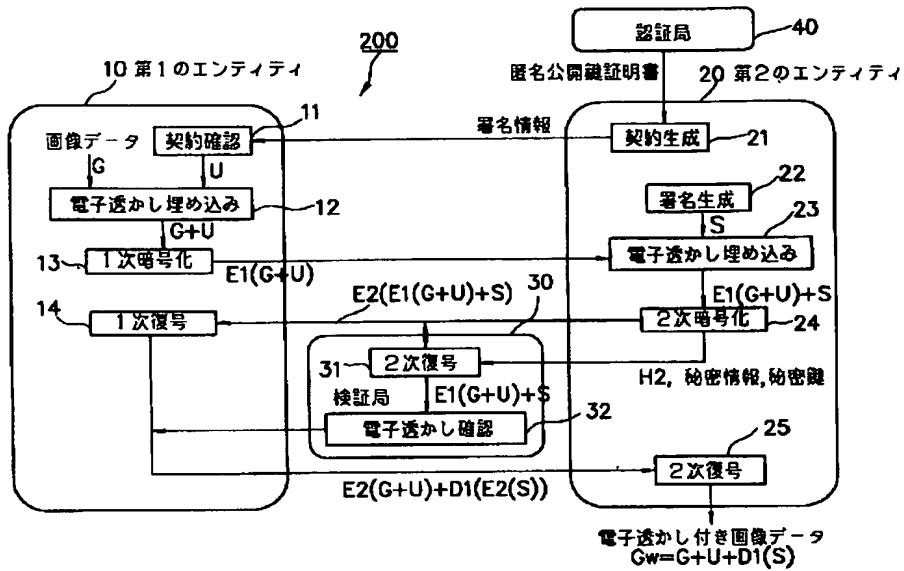
【図 1 2】

【図 1 3】

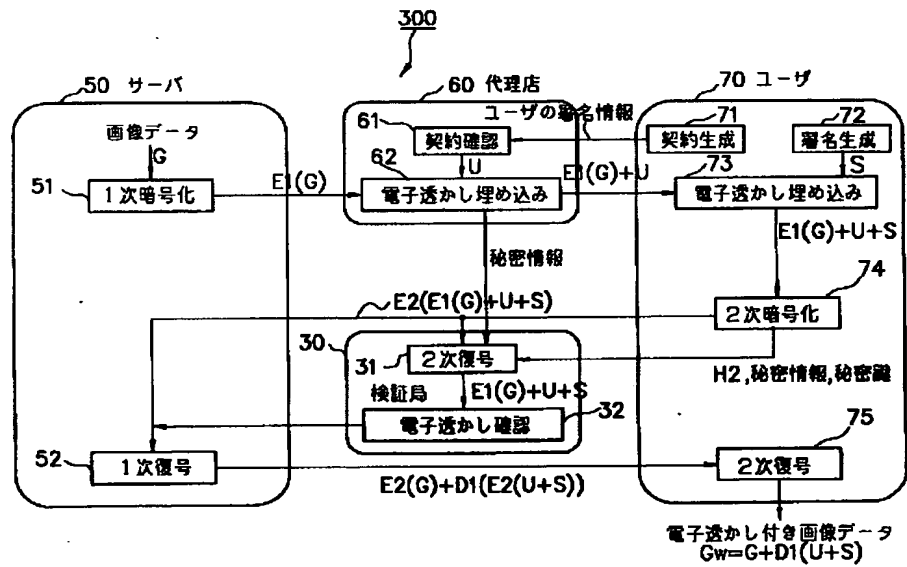
フィールド名	長さ	バイト
画像の幅	4	4-7
画像の高さ	4	8-11
タイルの総数	4	12-15
タイルの幅	4	16-19
タイルの高さ	4	20-23



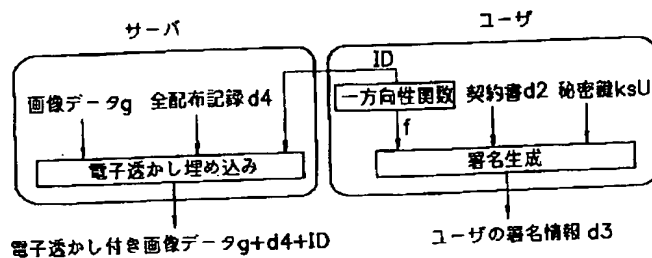
【図 2】



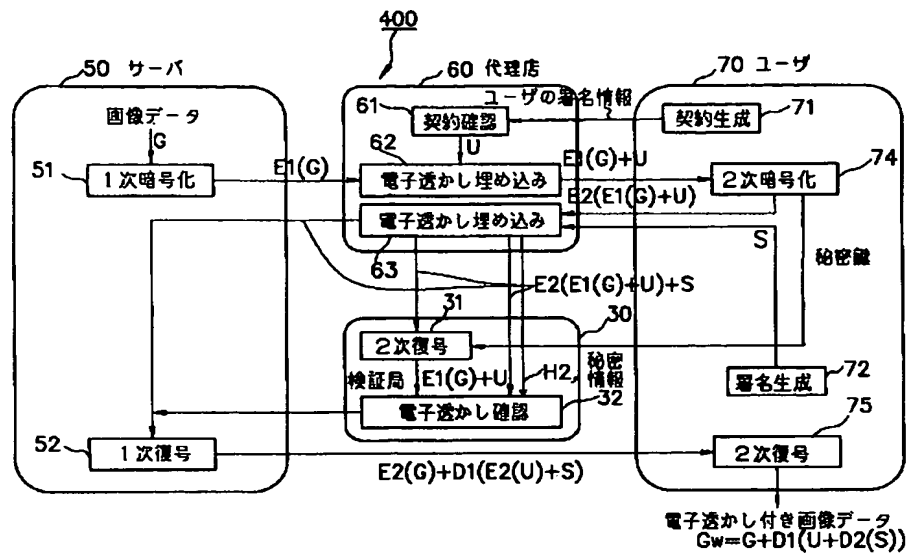
【図 3】



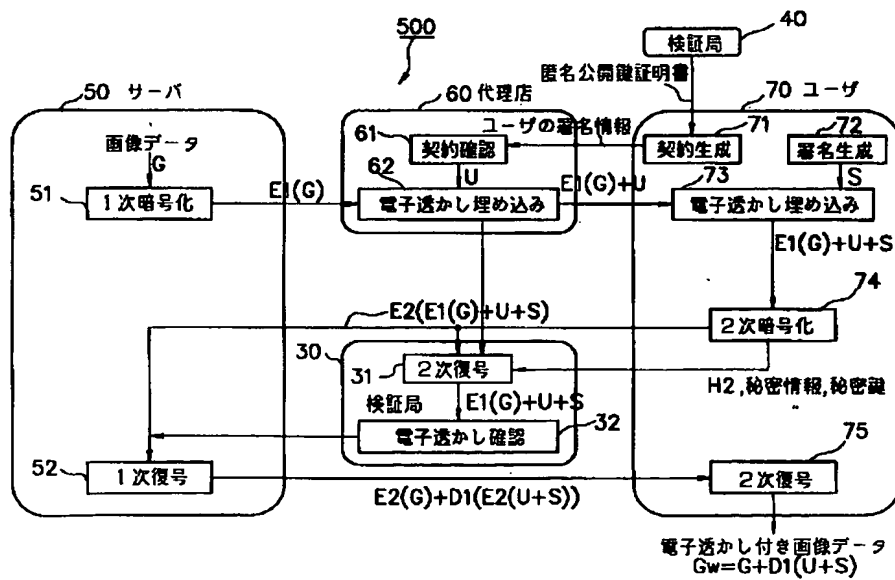
【図 1 4】



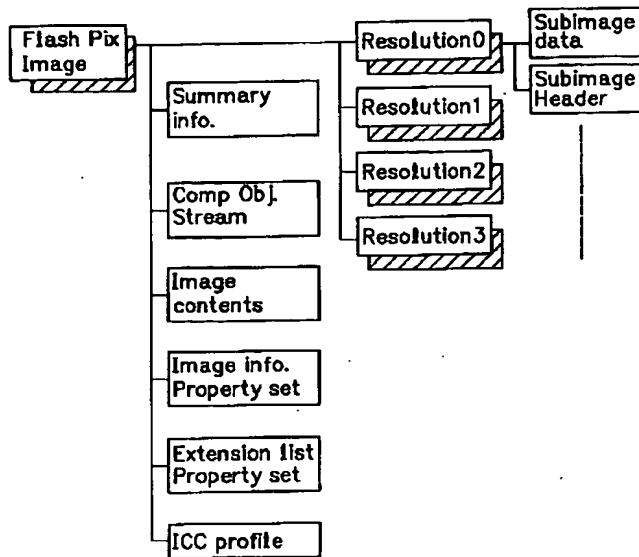
【図4】



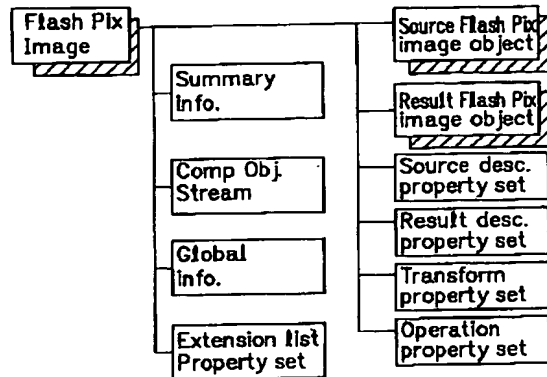
【図5】



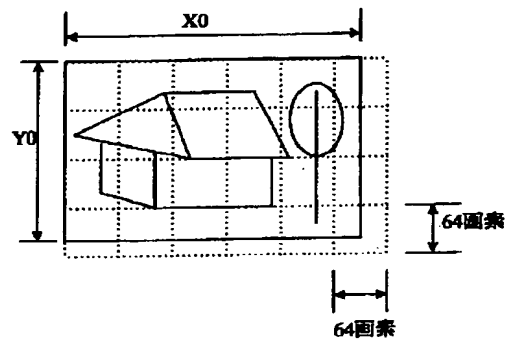
【図 7】



【図 8】



【図 1 1】



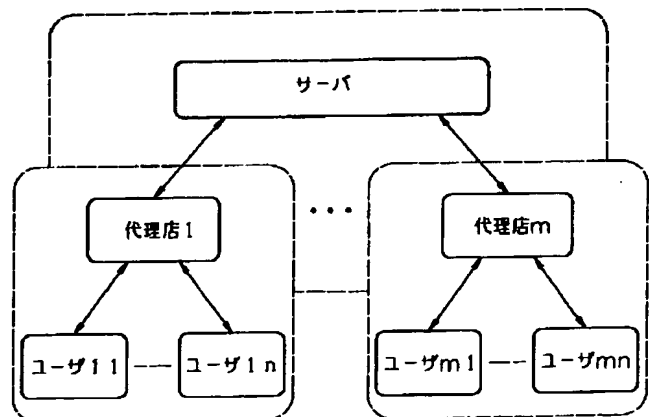
【図 9】

プロパティ名	IDコード	タイプ
画像データの階層数	0x01000000	VT_UI4
最大解像度の画像の幅	0x01000002	VT_UI4
最大解像度の画像の高さ	0x01000003	VT_UI4
初期表示の高さ	0x01000004	VT_R4
初期表示の幅	0x01000005	VT_R4

プロパティ名	IDコード	タイプ
各解像度の画像の幅	0x02ii0000	VT_UI4
各解像度の画像の高さ	0x02ii0001	VT_UI4
各解像度の画像の色	0x02ii0002	VT_BLOB
各解像度の画像を数値で表わしたフォーマット	0x02ii0003	VT_UI4 VT_VECTOR

プロパティ名	IDコード	タイプ
JPEGテーブル	0x03ii0001	VT_BLOB
最大JPEGテーブルのインデックス	0x03000002	VT_UI4

【図 1 6】



[illegible]

The diagram illustrates a network system architecture. At the center is a box labeled '代理店' (Agency). Above it, a row of boxes represents authors: '著作者1' (Author 1), '著作者2' (Author 2), an ellipsis '...', '著作者m-1' (Author m-1), and '著作者m' (Author m). Below the central box, a row of boxes represents users: 'ユーザ1' (User 1), 'ユーザ2' (User 2), an ellipsis '...', 'ユーザn-1' (User n-1), and 'ユーザn' (User n). Arrows point from each author box to the central '代理店' box, and from the central '代理店' box to each user box.

フロントページの続き

(51) Int. Cl. ⁶

識別記号

F I

H 0 4 N 7/081

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.